

METHOD AND SYSTEM FOR AUTHENTICATION OF A USER

ABSTRACT

5 A method and system for authentication of a user
(302, 402) by an authenticating entity (304, 404). The
method including the authenticating entity (304, 404)
sending a challenge (310, 410) to the user (302, 402).
The user (302, 402) adds a spoiler to the challenge (312,
412) and encrypts (316, 416) the combined spoiler and
challenge (314, 414) using a private key of an asymmetric
key pair. The user (302, 402) sends the encrypted
combined spoiler and challenge to the authenticating
entity (304, 404). The authenticating entity (304, 404)
ascertains that the returned challenge is the same the
original challenge (310, 410) and approves the user (302,
402).